

Village of Foxfire

IT Governance & Documentation Policy

Policy Number	IT-001
---------------	--------

Version Number	1.0
----------------	-----

Adopted By	
------------	--

Effective Date	
----------------	--

Policy Owner	Village Council
--------------	-----------------

Last Reviewed	
---------------	--

Next Scheduled Review	
-----------------------	--

IT Administrator	Daniel Horton – Horton Technical LLC
------------------	--------------------------------------

Village Administrator	Lisa Kievtt
-----------------------	-------------

1. Purpose

This policy establishes the framework by which the Village of Foxfire ("the Village") manages information technology credentials, assets, documentation, and personnel transitions. Prior to the appointment of the Village's first IT Administrator, no documented IT governance framework existed. This policy creates that foundational framework and governs the operational practices upon which all subsequent Village IT procedures depend.

2. Scope

This policy applies to all Village elected and appointed officials, employees, contractors, and volunteers who use, administer, or have access to Village-owned IT systems, accounts, credentials, hardware, or software. It covers all Village departments and facilities, including Village Administration, Village Water Department, the Police Department (subject to applicable CJIS standards), Village Park, and the Village Pool.

3. Policy Statements

3.1 Credential Management

- System of Record: The Village shall maintain a centralized, encrypted credential vault (password manager) as the sole authorized system of record for all shared and administrative IT credentials. Credentials shall not be stored in plaintext documents, spreadsheets, email, physical notes, or personal devices.

- **Migration & Inventory:** All existing shared credentials — including network equipment, NAS/backup systems, email administration, website/CMS, social media, camera/NVR systems, the FMS server, and Police Department infrastructure administered by Village IT — shall be inventoried and migrated into the vault.
- **Rotation:** Any credential previously shared or stored insecurely shall be rotated immediately upon discovery or migration into the vault.
- **Least Privilege:** Access to vaulted credentials shall grant each user or role the minimum access necessary to perform their duties.
- **Emergency Access ("Break-Glass"):** A documented emergency-access procedure shall be maintained to ensure continuity if the Village Administrator is unavailable. The physical or digital token required for this access shall be held securely by the Village Administrator or IT Administrator. Every invocation of emergency access must be logged, justified, and reviewed.
- **Auditing:** Credential vault contents and access logs shall be reviewed at least annually, and immediately following the departure of any staff member with administrative vault access.

3.2 IT Asset Inventory & Lifecycle

- **Living Inventory:** The Village shall maintain a living inventory of all IT hardware, software licenses, and support/warranty terms.
- **Hardware Tracking:** The hardware inventory shall record device type, make/model, serial number, assigned location/user, and acquisition date for all departments, including the Police Department.
- **Software & Compliance:** The software inventory shall record all active licenses, subscriptions, renewal dates, and costs to support compliance and budgeting.
- **Lifecycle & Disposal:** Warranty dates shall be tracked to inform replacement planning. No IT asset shall be disposed of, sold as surplus, or destroyed without the IT Administrator verifying certified data sanitization and updating the inventory log.
- **Audit Cadence:** The inventory shall be physically and digitally audited at least annually to confirm accuracy.

3.3 Documentation Standards

- **Infrastructure Mapping:** The Village shall maintain current-state physical and logical network diagrams, updated upon the completion of any major infrastructure project.
- **Standard Operating Procedures (SOPs):** SOPs shall be documented for recurring IT tasks, including user account lifecycle management, password resets, and backup restoration workflows.
- **Continuity of Access:** All governance documentation, diagrams, SOPs, and inventories shall be stored in a centralized, secure location accessible to the Village Administrator, independent of any individual's personal or local accounts.

3.4 Staff Onboarding & Offboarding

- **Onboarding:** A standardized IT onboarding checklist shall be executed for all new hires, covering account creation, email provisioning, hardware issuance, and mandatory Multi-Factor Authentication (MFA) enrollment.

- **Standard Offboarding:** A standardized offboarding checklist shall be executed for departing staff to ensure the return of hardware and the immediate revocation of system and physical access.
- **Involuntary/Immediate Offboarding:** In the event of an immediate or involuntary termination, the Village Administrator shall notify the IT Administrator if required, and system access shall be revoked concurrently with or prior to the termination action.
- **Notification:** The Village Administrator shall notify the IT Administrator in advance of any hire, departure, or role change if any specific access to systems needs to be revoked.

4. Roles & Responsibilities

Role	Responsibility
IT Administrator	Maintains the credential vault, asset inventory, and governance documentation. Executes onboarding/offboarding technical steps. Has access to "break-glass" emergency access.
Village Administrator	Notifies IT of personnel changes if required to revoke access to systems. Owns the "break-glass" emergency access.
Village Council	Adopts and formally reviews this policy; approves material changes.
All Authorized Users	Comply with credential handling requirements; report suspected security incidents or credential exposures immediately.

5. Enforcement

Failure to comply with this policy — including storing shared credentials outside the approved vault or bypassing onboarding/offboarding procedures — may result in revocation of system access and is subject to the Village's standard personnel or Village Councils disciplinary procedures.

6. Review Cycle

This policy shall be reviewed at least annually by the IT Administrator and revised as needed to reflect changes in Village systems, staffing, or applicable local and state legislation. Material revisions shall be presented to the Village Council for re-adoption.

7. Related Policies & Frameworks

This policy serves as the foundation for the following policy suites, to be developed and integrated sequentially:

- Acceptable Use & Cybersecurity Policy Suite
- Data Management, Retention, & Public Records Policy Suite
- Lifecycle, Asset Management, & Procurement Policy Suite
- Physical & Media Security Policy Suite

8. Definitions

Credential Vault: An encrypted, access-controlled password management platform used to store and share login credentials for shared/administrative accounts.

Break-Glass Procedure: A documented, auditable process for obtaining emergency access to credentials or systems outside of normal access channels.

Example: When to "Break the Glass"

- Imagine a locked emergency box containing master administrative override keys. Under normal circumstances, access requests follow standard approval channels. However, if a high-risk situation arises—such as a critical staff member being abruptly terminated or resigning—and the Village Administrator (who holds primary approval authority) is traveling and completely unreachable, waiting for normal authorization could leave sensitive municipal systems and data exposed to unauthorized access or retaliation.
- In this time-sensitive situation, the Village IT Administrator can "break the glass" to obtain emergency administrative credentials. This allows them to immediately revoke the departing employee's account access, disable active sessions, and secure the network. Once the procedure is activated, the system automatically logs who accessed the emergency credentials, exact timestamps, and every action taken—ensuring full accountability once the Village Administrator returns.

Least Privilege: The security principle of granting users the minimum level of access required to perform their job functions.

Adoption

Adopted by the Village of Foxfire Village Council on _____.

Signature: _____

Title: _____